Iranian Spear Phishing Operation Targets Former Israeli Foreign Minister, Former US Ambassador to Israel, Former Israeli Army General and Three other High-Profile Executives

By etal@ad.checkpoint.com

Published: 2022-06-14 · Archived: 2026-04-05 18:44:50 UTC

Check Point Research (CPR) exposes an Iranian spear-phishing operation targeting high-profile Israeli and US executives. The attackers hijacked emails of senior people in Israel and then used it to target other high-level officials to steal personal information. Targets have included former Israeli Foreign Minister, Tzipi Livni, the former US Ambassador to Israel, former Major General of the IDF, and three others. In addition, the attackers hijacked existing email exchanges and swapped emails to new ones, pretending to be someone else, to trick their targets into speaking to them. CPR believes the goal of the operation is to steal personal information, passport scans and access email accounts. CPR's findings come at time of rising tensions between Israel and Iran, where former attempts by Iran to lure Israeli targets via email have occurred.

Check Point Research (CPR) has exposed an Iranian spear-phishing operation targeting high-profile Israeli and US executives. As part of their operations, the attackers take over existing accounts of the executives and create fake impersonating accounts to lure their targets into long email conversations. CPR believes the goal of the operation is to steal personal information, passport scans, and access to email accounts. CPR sees that the operation dates to at least December 2021 but assumes earlier.

High profile targets include:

- **Tzipi Livni** – former Foreign Minister and Deputy Prime Minister of Israel
- **Former Major General** who served in a highly sensitive position in the IDF
- **Chair** of one of Israel's leading security think tanks
- **Former US Ambassador to Israel**
- **Former Chair** of a well-known Middle East research center
- **Senior executive** in the Israeli defense industry

Attack Methodology

1. The attacker takes over a real e-mail account of a frequent contact of the target
2. The attacker proceeds to hijack an existing email conversation
3. The attackers then open a fake email to impersonate the contact of the target, mostly in the format of .
4. The attackers continue the hijacked conversation from the fake email and exchanges at least several emails with the target
5. Some of the emails include a link to a real document that is relevant to the target. e.g, invitation to a conference or research / phishing page of Yahoo/ link to upload document scans

Example Emails: Tzipi Livni, Former Israeli Foreign Minister

Livni was approached via email by someone impersonating a well-known former Major General in the IDF who served in a highly sensitive position. The email was sent from his genuine email address which had previous correspondence with her in the past. The email contained a link to a file which the attacker requested her to open and read. When she delayed doing so, the attacker approached her several times asking her to open the file using her email password. This prompted her suspicions. When she met the former Major General and asked him about the email, it was confirmed that he never sent such an email to her.

Figure 1. Email to Tzipi Livni on Day 1

Translated

Figure 2. Email to Tzipi Livni on Day 6

Translated

Attribution

CPR believes that the threat actors behind the operation are an Iranian-backed entity. Evidence points to a possible connection of the operation to the Iran-attributed Phosphorus APT group. The group has a long history of conducting high-profile cyber operations, aligned with the interest of the Iranian regime, as well as targeting Israeli officials.

How to Recognize Phishing Emails

Phishers use a wide range of techniques to make their phishing emails look legitimate. These are some of the most used techniques, which can be used to identify these malicious emails.

Psychological Tricks

Phishing emails are designed to convince the recipient to do something that is not in their best interests (giving away sensitive information, installing malware, etc.). To accomplish this, phishers commonly use psychological tricks in their campaigns, such as:

- Sense of Urgency: Phishing emails commonly tell their recipients that something needs to be done right away. This is because someone in a hurry is less likely to think about whether the email looks suspicious or is legitimate.
- Use of Authority: Business email compromise (BEC) scams and other spear-phishing emails commonly pretend to be from the CEO or someone else in authority. These scams take advantage of the fact that the recipient is inclined to follow orders from their bosses.
- Fear and Blackmail: Some phishing emails threaten consequences (such as revealing allegedly stolen sensitive data) if the recipient doesn't do what the attacker says. The fear of embarrassment or punishment

convinces the recipient to comply.

If an email seems coercive in any way, it might be a phishing attack.

Suspicious Requests

Phishing emails are designed to steal money, credentials, or other sensitive information. If an email makes a request or a demand that seems unusual or suspicious, then this might be evidence that it is part of a phishing attack.

Fake Domains

One of the most common techniques used in phishing emails are lookalike or fake domains. Lookalike domains are designed to appear to be a legitimate or trusted domain at a casual glance. For example, instead of the email address , a phishing email may use . While these emails may look like the real thing, they belong to a completely different domain that may be under the attacker's control.

What to Do if You Suspect a Phishing Attack

The impact and cost of a phishing attack on an organization depends on the speed and correctness of its response. If you suspect that an email may be a phishing email, take the following steps:

1. Don't Reply, Click Links, or Open Attachments: Never do what a phisher wants. If there is a suspicious link, attachment, or request for a reply don't click, open, or send it.
2. Report the Email to IT or Security Team: Phishing attacks are commonly part of distributed campaigns, and just because you caught the scam doesn't mean that everyone did. Report the email to IT or the security team so that they can start an investigation and perform damage control as quickly as possible.
3. Delete the Suspicious Email: After reporting, delete the suspicious email from your Inbox. This lessens the chance that you'll accidentally click on it without realizing it later.
4. While awareness of common phishing tactics and knowledge of anti-phishing best practices is important, modern phishing attacks are sophisticated enough that some will always slip through. Phishing awareness training should be supplemented with anti-phishing solutions that can help to detect and block attempted phishing campaigns. Check Point Harmony Email & Office provides visibility and protection across email phishing techniques. To learn more about protecting your organization against phishing emails, please request a free demo.

Conclusion

The Iranian-affiliated Phosphorous APT group continues its spear-phishing activity against targets of the Iranian regime. This research has exposed Iranian phishing infrastructure that targets Israeli and US public sector executives, with the goal to steal their personal information, passport scans, and steal access to their mail accounts. CPR researchers have solid evidence this operation dates back to December 2021 but could have started even earlier. The most sophisticated part of the operation is the social engineering. The attackers use real hijacked email chains, impersonations to well-known contacts of the targets and specific lures for each target. The operation implements a very targeted phishing chain that is specifically crafted for each target. In addition, the

aggressive email engagement of the nation state attacker with the targets is rarely seen in the nation state cyber-attacks. CPR will continue to monitor the operation.

For more detailed technical information and examples of the operation you can read the technical blog

---